Remarks

Status of the Claims

Claims 1-5, 11-21, and 23 are pending in the application. All claims stand rejected. The pending claims have not been amended herein. For the reasons set forth below, The Applicants submit that each of the pending claims is patentably distinct from the cited prior art and in condition for allowance. Reconsideration of the claims is therefore respectfully requested.

Claim Rejections - 35 U.S.C. § 103

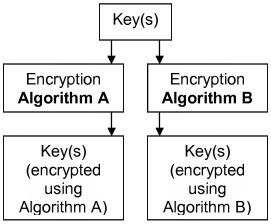
Claims 1, 3-5, 11-12, and 14-16 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Patent No. 6,690,795 to Richards ("Richards") in view of Peacock, "Features and Utilization of Motorola's Advanced INFOSEC Machine, AIM, in Embedded Encryption Applications" ("Peacock"); claims 2, 13 and 17-20 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Richards in view of Peacock and in further view of U.S. Patent No. 6,415,031 issued to Colligan Jr., et al. ("Colligan"); claim 21 stands rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Richards in view of U.S. Patent No. 6,598,231 issued to Basawapatna ("Basawapatna"); and claim 23 stands rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable Richards in view of Basawapatna and in further view of Colligan. These rejections are respectfully traversed. As set forth below, the Applicants respectfully submit that each of the pending claims is patentably distinct from the cited references, individually and collectively.

Specifically, as discussed in detail below, the combination of Richards and Peacock merely teaches encrypting a key using a single algorithm, and eventually updating that single algorithm by programming both old and new algorithms into a multi-processor cryptography chip when transitioning from older, legacy systems to new systems. Applicants respectfully submit, however, that the combination of Richards and Peacock fails to teach ***concurrently transmitting*** a key (or group of keys) that is encrypted ***twice using two different algorithms***.

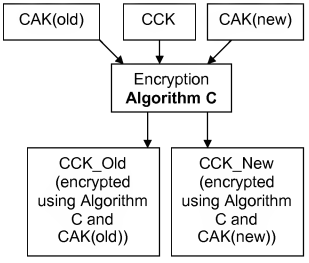
As discussed in Applicants' previous responses, an aspect of the pending claims is that a group of original multimedia channel keys are encrypted using a first encryption algorithm decryptable by a first multimedia receiver. The same group of original multimedia channel keys are also encrypted using a second encryption algorithm decryptable by a second multimedia receiver. The two groups of encrypted keys are then concurrently transmitted. Thus, receivers with newer and more advanced types of encryption may be introduced into the market without discontinuing service to older receivers.

Richards teaches changing a channel access key (CAK) each month to a different code so as to allow channel access to customers who continue to pay their bills. Col. 14, lines 39-49. The CAK is used to encrypt/decrypt a control channel key (CCK). See FIG. 14 and col. 11, lines 14-21. New CAKs cannot be delivered to all customers instantaneously, thus a transition period is provided when both old and new CAKs are used with a single algorithm to encrypt a CCK. Col. 16, lines 51-53, and col. 17, lines 7-13 and 36-43. The drawings below illustrate the difference in using two

different encryption algorithms (as required by the pending claims) and using two different encryption keys (as taught by Richards).



Pending Claims
(*two algorithms*)



Richards
(two keys (CAK), *one algorithm*)

As illustrated above, encrypting a key (or group of keys) using two different algorithms is clearly different than encrypting a key (CCK) using a single algorithm with two different encryption keys (CAK(old) and CAK(new)). An encryption algorithm typically transforms data based on a code referred to as a key. Thus, a single type of encryption may select from a large number of potential codes (keys) to encrypt/decrypt data according to a single algorithm. While Richards teaches changing the code (CAK) on a monthly basis, Richards is silent as to changing the underlying ***algorithm*** used to encrypt/decrypt the data.

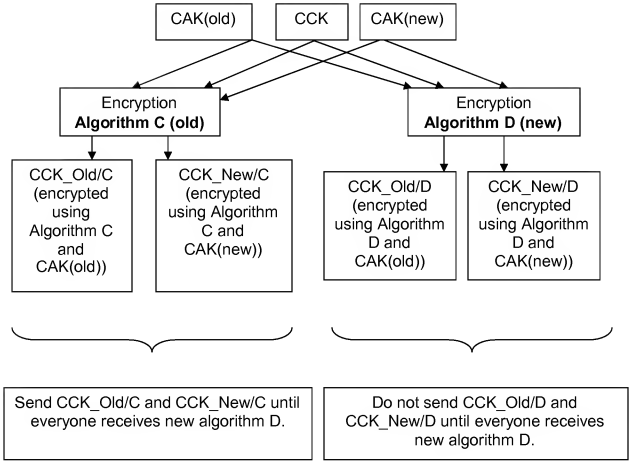
Peacock does not remedy the deficiencies of Richards. Peacock discloses a multi-processor cryptographic chip that can run multiple algorithms on multiple channels. See, *e.g.*, the Abstract on page 423 and the "Crypto Processors" on page

425. The multi-processor cryptographic chip allows for "new crypto devices and algorithms operating at different levels of security." Introduction on page 423.

Pages 428 and 429 of Peacock discuss applications for the multi-processor cryptographic chip, including "legacy replacement/transition." Because the chip can process multiple algorithms simultaneously (see page 425, col. 2), pages 3 and 4 of the Office Action assert that "Peacock further teaches that during the transition phase the chip disclosed is capable of executing both the first and the second encryption algorithm." However, being able to simultaneously run multiple algorithms does not by itself mean that the same group of keys would be ***concurrently transmitted*** (*e.g.*, by a head-end of a cable or satellite provider) to a receiver (*e.g.*, a set-top-box).

Rather, the conventional method for transitioning from legacy systems to new systems is to start updating each set-top-box with a new algorithm. The head-end continues transmitting content encrypted using the old algorithm until all of the set-top-boxes have been updated with the new algorithm, at which time the head-end starts transmitting content encrypted using the new algorithm. Because the set-top-boxes have both algorithms, they can immediately start decrypting using the new algorithm once the head-end finally starts to transmit content encrypted with the new algorithm. As indicated on page 429 of Peacock, the disclosed chip is useful for such a scenario because it "***can be programmed*** to execute both the old and new algorithms." (Emphasis added). Peacock is silent, however, with regards to ***concurrently transmitting*** content encrypted using both old and new algorithms.

The drawing below illustrates the combination of Richards with Peacock:



Richards + Peacock
(Still does not concurrently transmit the same group of keys encoded twice using two different algorithms.)

As illustrated, the combination of Richards with Peacock still fails to teach concurrently transmitting a key (or group of keys) that is encrypted twice using two different algorithms. Rather, the combination transmits ***either*** CCK_Old/C and CCK_New/C, **or** CCK_Old/D and CCK_New/D. Either way, the combination ***transmits*** the key CCK encrypted using a ***single algorithm at a time*** and two different keys (CAK(old) and CAK(new)).

For at least the foregoing reasons, the cited prior art references, whether considered individually or in combination, fail to disclose each of the limitations in any of the pending independent claims. For at least the same reasons, each of the claims depending therefrom are also patentably distinct from the cited prior art.

In view of the foregoing, all pending claims represent patentable subject matter. A Notice of Allowance is respectfully requested.

Respectfully submitted,

Digeo, Inc.

By /Kory D. Christensen/
Kory D. Christensen
Registration No. 43,548

STOEL RIVES LLP
One Utah Center Suite 1100
201 S Main Street
Salt Lake City, UT 84111-4904
Telephone: (801) 328-3131
Facsimile: (801) 578-6999